IHK Erfurt: Hintergründe zum deutschlandweiten Hackerangriff auf die IHK

Erfurt. Am 3. August 2022 schaltete die IHK-GfI, IT-Dienstleister der IHK-Organisation, die bei ihr gehosteten IT-Systeme der IHK Erfurt ab. Dadurch ging die Webseite der IHK offline und die Mitarbeitenden waren nicht mehr per E-Mail erreichbar. Verschiedene interne und externe Software-Anwendungen der IHK funktionierten nicht mehr. In unterschiedlicher Form waren die IT-Systeme aller 79 Industrie- und Handelskammern in Deutschland betroffen. Wie aktuelle Erkenntnisse nun zeigen, war dies der richtige Schritt, um die IHK Erfurt und ihre Mitgliedsunternehmen vor gravierenden Schäden zu bewahren. Hinter dem Cyber-Angriff stecken nach Erkenntnissen der IT-Forensiker extrem professionelle Hacker. Die Vorgehensweise der Hacker deutet auf einen Angriff zum Zweck der Spionage oder Sabotage hin, auch wenn sich ein finanziell motivierter Hintergrund des Angriffs noch nicht ausschließen lässt.

Von langer Hand vorbereitet

Die IHK-GfI entdeckte am 3. August 2022 ein auffälliges Verhalten in ihren IT-Systemen. Die Experten des IHK Cyber Emergency Response Teams (IHK-CERT) der IHK-GfI haben den Vorfall daraufhin unverzüglich untersucht. In Zusammenarbeit mit externen IT-Sicherheitsexperten entschied die IHK-GfI, aus Sicherheitsgründen die Verbindung aller Industrie- und Handelskammern zum Internet zu trennen. Ein solches Vorgehen verwehrt Angreifern den weiteren Zugriff auf die Systeme und verhindert somit eine weitere Fortführung des Angriffs, insbesondere den Diebstahl oder die mögliche Verschlüsselung von Daten. Dadurch konnte die IHK-GfI den Angriff stoppen. Wie die IHK-GfI nun aktuell mitteilt, zeigen die Ergebnisse der IT-Forensik, dass der Angriff von langer Hand vorbereitet wurde. Die von den Hackern eingesetzten Werkzeuge zur Manipulation sind hochentwickelt.

Angriff erkannt und aufgehalten

Nach Einschätzung der externen Experten reagierte die IHK-GfI konsequent und unter dem Gesichtspunkt der wirtschaftlichen und politischen Rahmenbedingungen und aus der Erfahrung aus vergleichbaren Vorfällen absolut angemessen. Aufgrund der Professionalität und Diskretion der Hacker bewertet die IHK-GfI das Risiko weiterer Angriffe als hoch. Daher werden die Software-Anwendungen und IT-Systeme der IHKs nur nach intensiver Prüfung schrittweise hochgefahren. Bis alle Industrie- und Handelskammern deutschlandweit wieder voll funktionsfähig arbeiten können, wird es folglich noch einige Wochen dauern. Dies gilt auch für die IHK Erfurt. Zwar ist die Webseite zu großen Teilen wiederhergestellt. Bis die IHK-Mitgliedsunternehmen jedoch wieder vollständig auf die digitalen Services zugreifen können, wird es noch dauern. Trotzdem ist die IHK voll arbeitsfähig.

Mitgliedsunternehmen können sich bei aktuellen Anliegen an folgende Kontakte wenden: E-Mail: ihk.erfurt-notfall@posteo.de oder medien.ihk.erfurt-notfall@posteo.de. Telefonnummer: 0361 – 34 84 292 (Zentrale). Website: www.ihk.de/erfurt

Gefahr von Trittbrettfahrern

Außerdem warnen die IHK Erfurt und die IHK-GfI ausdrücklich vor Trittbrettfahrern. Der Bekanntheitsgrad des Vorfalls ruft mit hoher Wahrscheinlichkeit weitere Kriminelle auf den Plan: Diese könnten Phishing, Social-Engineering und andere Methoden einsetzen, um von der Situation zu profitieren. Daher sollte man besonders wachsam sein im Umgang mit (vermeintlichen) E-Mails der IHK. Zuletzt verschickten Kriminelle beispielsweise Phishing-E-Mails, die Mitgliedsunternehmen aufforderten, sich „neu zu identifizieren“, ansonsten würde der jeweilige Account nach einer gewissen Frist gesperrt werden. Wenn Zweifel bestehen, ob eine E-Mail tatsächlich aus der IHK stammt, so sollte zur Absicherung eine kurze telefonische Klärung stattfinden.